



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/915,511	07/26/2001	Michael Wayne Brown	AUS920010528US1	6703
7590	01/25/2005		EXAMINER	
Marilyn Smith Dawkins International Business Machines Corporation Intellectual Property Law Department 11400 Burnet Road., Internal Zip 4054 Austin, TX 78758			WILLIAMS, JEFFERY L	
			ART UNIT	PAPER NUMBER
			2137	
			DATE MAILED: 01/25/2005	

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/915,511	BROWN ET AL.	
	Examiner	Art Unit	
	Williams Jeffery	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on _____.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-38 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 28 September 2001 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____. |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>7-26-01</u> . | 6) <input type="checkbox"/> Other: _____. |

Art Unit: 2137

Remarks

Claims 1 – 38 are pending.

The applicants are requested to amend the Cross-Reference to Related

Applications to:

- (1) clearly identify each application by serial number and filing date, and
 - (2) remove any reference to the attorney docket number.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 5, 7 – 9, 11 – 13, 15 – 17, 19 – 21, 23 – 25, and 27 - 38 are rejected

under 35 U.S.C. 103(a) as being unpatentable over DeSimone et al., US Patent:

6,212,548 B1 in view of Smithies et al., US Patent: 6,091,835.

25

Art Unit: 2137

1 Regarding claim 1, DeSimone et al. discloses a method for enabling a
2 messaging session comprising a plurality of users participating in the session. The
3 participating users are able to view the history of the messaging session in the form of a
4 'conversation', a string of recorded messages (Col. 2, lines 48-56; Col. 3, lines 43-53).
5 DeSimone et al. does not disclose that the messaging session is verifiable by attaching
6 digital signatures of the participants to the recording of the session. DeSimone et al.,
7 however, does teach the understanding that certain messaging sessions between users
8 may need measures of security provided (Col. 14, lines 50-54).

9 Smithies et al. discloses a method for recording a verifiable transcript of
10 statements, transactions, or events between parties by attaching digital signatures of
11 the participants to the transcript (Col. 3, lines 40-61; Col. 41, lines 21-36).

12 To combine the method for enabling a messaging session and a history of the
13 session between participants with a method for recording digital signatures of
14 participants along with the transcript would provide a needed measure of security.
15 Therefore, it would have been obvious to one ordinarily skilled in the art to combine the
16 method of DeSimone et al. with the method of Smithies et al., because it is obvious that
17 certain messaging sessions between users will require the level of verifiability and
18 accountability that a digitally signed transcript would provide.

19
20 Regarding claim 2, the combination of DeSimone et al. and Smithies et al.
21 discloses the recording of the selection of message entries and attaching the plurality of
22 digital signatures at a messaging server system connected via a network to a plurality of

Art Unit: 2137

1 client systems accessible to the plurality of users (Smithies et al., Fig. 2, Col. 3, lines
2 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the
3 transcript generator module may reside on a system other than a client system that has
4 access to it. In this case, digital signatures from a plurality of interacting client systems
5 will be attached at the messaging server system.

6

7 Regarding claim 3, the combination of DeSimone et al. and Smithies et al.
8 discloses the recording of the selection of message entries and attaching the plurality of
9 digital signatures at a client system connected via a network to a plurality of client
10 systems accessible to the plurality of users (Smithies et al., Fig. 1, Col. 3, lines 40-61;
11 Col. 8, lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client
12 application and the transcript generator module both reside on the client system, then
13 the digital signatures will be attached at the client system.

14

15 Regarding claim 4, the combination of DeSimone et al. and Smithies et al.
16 discloses a method for verifying a messaging session, wherein verifying includes at
17 least one of verifying at least one of a plurality of digital signatures and verifying an
18 integrity of the messaging session (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col.
19 11, lines 44-67). As disclosed by Smithies et al., the transcript generator module will
20 perform session verification functions upon the transcript, such as verification of
21 signatures and verification of the transcript checksum.

22

1 Regarding claim 5, the combination of DeSimone et al. and Smithies et al.
2 discloses a method for transmitting a request to a plurality of users to each attach a
3 digital signature to a recording of a selection of message entries from a messaging
4 session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines 46-56). As disclosed by
5 Smithies et al., multiple parties, or users, can engage in the generation of a transcript.
6 The transcript generator module will request participants to the session to provide their
7 digital signatures to the transcript.

8

9 Regarding claim 7, the combination of DeSimone et al. and Smithies et al.
10 discloses a method for calculating a checksum for the recording of the selection of
11 message entries from the messaging session; and encrypting the checksum utilizing a
12 private key for a particular digital signature from among the plurality of digital signatures,
13 wherein a particular public key is enabled to decrypt the encrypted checksum (Smithies
14 et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

15

16 Regarding claim 8, the combination of DeSimone et al. and Smithies et al.
17 discloses a method for verifying an integrity of a selection of message entries by
18 calculating a current checksum for the selection of the plurality of message entries;
19 decrypting said encrypted checksum with a particular public key; and comparing the
20 current checksum with the decrypted checksum, wherein the integrity is verified if the
21 decrypted checksum matches the current checksum (Smithies et al., Col. 14, lines 26-
22 39).

Art Unit: 2137

1
2 Regarding claim 9, the combination of DeSimone et al. and Smithies et al.
3 discloses a method for verifying a particular digital signature from among a plurality of
4 digital signatures in order to verify a particular user from among a plurality of users
5 associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13, 21-
6 36).

7
8 Regarding claim 11, DeSimone et al. discloses a system for recording a
9 message session comprising a server system communicatively connected to a network
10 (Col. 3, line 43 – Col. 4, line 18). DeSimone et al. does not disclose the server system
11 comprising means to record the selection of message entries and means for attaching
12 the digital signatures of the session participants to the recording of the selection of
13 message entries.

14 Smithies et al. discloses means to record a transcript (the selection of message
15 entries from the plurality of users) as well as a means for attaching the digital signatures
16 of the session participants to the recording of the selection of message entries (Col. 7,
17 lines 41-50; Col. 24, lines 48-55; Col. 41, lines 24-35; Col. 41, line 64 - Col. 42, line 37).
18 As disclosed by Smithies et al., communicating parties can digitally sign a transcript,
19 generated by a transcript generator module that is residing on a server.

20 The combination of the methods of DeSimone et al. and Smithies et al., as
21 explained regarding claim 1, would obviously be utilized in a system. Thus, it would
22 have been obvious to one ordinarily skilled in the art to combine the system of

Art Unit: 2137

1 DeSimone et al. with the system of Smithies et al., because it is obvious that certain
2 systems that record messaging sessions between users will require the level of
3 verifiability and accountability that a system utilizing a digitally signed transcript would
4 provide.

5

6 Regarding claim 12, the combination of DeSimone et al. and Smithies et al.
7 discloses a logging controller for verifying a messaging session, wherein the verifying
8 includes at least one of verifying at least one of a plurality of digital signatures and
9 verifying an integrity of the messaging session (Smithies et al., Col. 9, line 64 – Col. 10,
10 line 9; Col. 11, lines 44-67). As disclosed by Smithies et al., the transcript generator
11 module will perform session verification functions upon the transcript, such as
12 verification of signatures and verification of the transcript checksum.

13

14 Regarding claim 13, the combination of DeSimone et al. and Smithies et al.
15 discloses a system means for transmitting a request to a plurality of users to each
16 attach a digital signature to a recording of a selection of message entries from a
17 messaging session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines 46-56). In the
18 system, as disclosed by Smithies, multiple parties, or users, can engage in the
19 generation of a transcript. The transcript generator module will request participants to
20 the session to provide their digital signatures to the transcript.

21

Art Unit: 2137

1 Regarding claim 15, the combination of DeSimone et al. and Smithies et al.
2 discloses a system means for calculating a checksum for the recording of a selection of
3 message entries from a messaging session; and means for encrypting a checksum
4 utilizing a private key for a particular digital signature from among a plurality of digital
5 signatures, wherein a particular public key is enabled to decrypt the encrypted
6 checksum (Smithies et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

7

8 Regarding claim 16, the combination of DeSimone et al. and Smithies et al.
9 discloses a system means for verifying an integrity of a selection of a plurality of
10 message entries by calculating a current checksum for the selection of the plurality of
11 message entries; decrypting said encrypted checksum with a particular public key; and
12 comparing the current checksum with the decrypted checksum, wherein the integrity is
13 verified if the decrypted checksum matches the current checksum (Smithies et al., Col.
14 14, lines 26-39).

15

16 Regarding claim 17, the combination of DeSimone et al. and Smithies et al.
17 discloses a system means for verifying a particular digital signature from among a
18 plurality of digital signatures in order to verify a particular user from among a plurality of
19 users associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13,
20 21-36).

21

1 Regarding claim 19, DeSimone et al. discloses both a method and system
2 implementing the method for recording a message session, as explained in claims 1
3 and 11. DeSimone et al. does not directly disclose the system utilizing a method that
4 has been implemented in a program residing on a computer readable medium.

5 Smithies et al. discloses a program means for enabling a recording of a transcript
6 (the selection of message entries from the plurality of users) as well as a program
7 means for attaching the digital signatures of the session participants to the recording of
8 the selection of message entries (Col. 7, lines 41-50; Col. 24, lines 48-55; Col. 41, lines
9 24-35; Col. 41, line 64 - Col. 42, line 37). As disclosed by Smithies et al.,
10 communicating parties can digitally sign a transcript by running browser software
11 enhanced by Java code downloaded from a server.

12 The combination of the methods/systems of DeSimone et al. and Smithies et al.,
13 as explained regarding claims 1 and 11, would obviously incorporate a program means
14 and a computer readable medium embodied by the program means. Thus, it would
15 have been obvious to one ordinarily skilled in the art to combine the system/method
16 means of DeSimone et al. with the system/method/program means of Smithies et al.,
17 because it is obvious that systems utilizing methods for recording messaging sessions
18 between users will require program means for practical implementation.

19
20 Regarding claim 20, the combination of DeSimone et al. and Smithies et al.
21 discloses program means for enabling verification of a messaging session, wherein
22 verifying includes at least one of verifying at least one of a plurality of digital signatures

1 and verifying an integrity of the messaging session. (Smithies et al., Col. 9, line 64 –
2 Col. 10, line 9; Col. 11, lines 44-67). As disclosed by Smithies et al., the transcript
3 generator module will perform session verification functions upon the transcript, such as
4 verification of signatures and verification of the transcript checksum. Further, as
5 disclosed by Smithies et al., with reference to claim 19, the transcript generator module
6 and other supporting system components are implemented as programs.

7

8 Regarding claim 21, the combination of DeSimone et al. and Smithies et al.
9 discloses a program means for controlling transmission of a request to a plurality of
10 users to each attach a digital signature to a recording of said selection of message
11 entries from a messaging session. (Smithies et al., Col. 41, lines 21-36, Col. 44, lines
12 46-56). In the program means, as disclosed by Smithies et al., multiple parties, or
13 users, can engage in the generation of a transcript. The transcript generator module
14 will request participants to the session to provide their digital signatures to the transcript.

15

16 Regarding claim 23, the combination of DeSimone et al. and Smithies et al.
17 discloses a program means for calculating a checksum for a recording of a selection of
18 message entries from a messaging session; and means for enabling encryption of the
19 checksum utilizing a private key for a particular digital signature from among a plurality
20 of digital signatures, wherein a particular public key enabled to decrypt the encrypted
21 checksum (Smithies et al., Col. 8, lines 24-43; Col. 14, lines 26-39).

1 Regarding claim 24, the combination of DeSimone et al. and Smithies et al.
2 discloses a program means for verifying an integrity of a selection of a plurality of
3 message entries by calculating a current checksum for the selection of the plurality of
4 message entries; decrypting said encrypted checksum with a particular public key; and
5 comparing the current checksum with the decrypted checksum, wherein the integrity is
6 verified if the decrypted checksum matches the current checksum (Smithies et al., Col.
7 14, lines 26-39).

8

9 Regarding claim 25, the combination of DeSimone et al. and Smithies et al.
10 discloses a program means for verifying a particular digital signature from among a
11 plurality of digital signatures in order to verify a particular user from among a plurality of
12 users associated with the particular digital signature (Smithies et al., Col. 41, lines 7-13,
13 21-36).

14

15 Regarding claim 27, the combination of DeSimone et al. and Smithies et al.
16 discloses a method for attaching a digital signature for a sender of a message entry to
17 the message entry; and distributing the message entry to a plurality of participants in a
18 messaging session, wherein each of the plurality of participants in the messaging
19 session are enabled to verify the message entry with the digital signature in real-time
20 (Smithies et al., Col. 13, lines 14-51; Col. 12, lines 14-16, 51-54; Col. 14, line 65 – Col.
21 15, line 4; Col. 41, lines 24-36). As disclosed by Smithies et al., messages created by
22 an individual through a client application are ‘affirmed’ (i.e. digitally signed) by the

1 individual. They are then added to the transcript, where other participants through their
2 respective client applications can view the transcript of messages, verify signatures of
3 the messages, and add their own messages.

4

5 Regarding claim 28, the combination of DeSimone et al. and Smithies et al.
6 discloses a method for attaching a digital signature for a sender at a client messaging
7 system before distribution within a network (Smithies et al., Fig. 1, Col. 8, lines 15-40;
8 Col. 41, lines 21-36). As shown by Smithies et al., when the client application and the
9 transcript generator module both reside on the client system, then the digital signatures
10 will be attached at the client system.

11

12 Regarding claim 29, the combination of DeSimone et al. and Smithies et al.
13 discloses a method for attaching a digital signature for a sender at a messaging server
14 before distribution to a plurality of participants (Smithies et al., Fig. 2, Col. 3, lines 40-61;
15 Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the transcript
16 generator module may reside on a system other than a client system that has access to
17 it. In this case, digital signatures from a plurality of interacting client systems will be
18 attached at the messaging server system.

19

20 Regarding claim 30, the combination of DeSimone et al. and Smithies et al.
21 discloses a method for verifying at least one of an identity of a sender and an integrity of
22 content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11,

Art Unit: 2137

1 lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As disclosed by
2 Smithies et al., a user via a client application can utilize the transcript generator module
3 to perform session verification functions upon the transcript, such as verification of
4 statements ('message entries') and their corresponding signatures.

5

6 Regarding claim 31, the combination of DeSimone et al. and Smithies et al.
7 discloses a messaging system means for attaching a digital signature for a sender of a
8 message entry to the message entry; and means for distributing the message entry to a
9 plurality of participants in a messaging session, wherein each of the plurality of
10 participants in the messaging session are enabled to verify the message entry with the
11 digital signature in real-time (Smithies et al., Col. 13, lines 14-51; Col. 12, lines 14-16,
12 51-54; Col. 14, line 65 – Col. 15, line 4; Col. 41, lines 24-36). As disclosed by Smithies
13 et al., messages created by an individual through a client application are 'affirmed' (i.e.
14 digitally signed) by the individual. They are then added to the transcript, where other
15 participants through their respective client applications can view the transcript of
16 messages, verify signatures of the messages, and add their own messages.

17

18 Regarding claim 32, the combination of DeSimone et al. and Smithies et al.
19 discloses a system means for attaching a digital signature for a sender at a client
20 messaging system before distribution within a network (Smithies et al., Fig. 1, Col. 8,
21 lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client

Art Unit: 2137

1 application and the transcript generator module both reside on the client system, then
2 the digital signatures will be attached at the client system.

3

4 Regarding claim 33, the combination of DeSimone et al. and Smithies et al.
5 discloses a system means for attaching a digital signature for a sender at a messaging
6 server before distribution to a plurality of participants (Smithies et al., Fig. 2, Col. 3, lines
7 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies et al., the
8 transcript generator module may reside on a system other than a client system that has
9 access to it. In this case, digital signatures from a plurality of interacting client systems
10 will be attached at the messaging server system.

11

12 Regarding claim 34, the combination of DeSimone et al. and Smithies et al.
13 discloses a system means for verifying at least one of an identity of a sender and an
14 integrity of content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line
15 9; Col. 11, lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As
16 disclosed by Smithies et al., a user via a client application can utilize the transcript
17 generator module to perform session verification functions upon the transcript, such as
18 verification of statements ('message entries') and their corresponding signatures.

19

20 Regarding claim 35, the combination of DeSimone et al. and Smithies et al.
21 discloses a program means for enabling attachment of a digital signature for a sender of
22 a message entry to the message entry; and means for controlling distribution of the

Art Unit: 2137

1 message entry to a plurality of participants in a messaging session, wherein each of the
2 plurality of participants in the messaging session are enabled to verify the message
3 entry with the digital signature in real-time (Smithies et al., Col. 13, lines 14-51; Col. 12,
4 lines 14-16, 51-54; Col. 14, line 65 – Col. 15, line 4; Col. 41, lines 24-36). As disclosed
5 by Smithies et al., messages created by an individual through a client application are
6 ‘affirmed’ (i.e. digitally signed) by the individual. They are then added to the transcript,
7 where other participants through their respective client applications can view the
8 transcript of messages, verify signatures of the messages, and add their own
9 messages.

10

11 Regarding claim 36, the combination of DeSimone et al. and Smithies et al.
12 discloses a program means for enabling attachment of a digital signature for a sender at
13 a client messaging system before distribution within a network (Smithies et al., Fig. 1,
14 Col. 8, lines 15-40; Col. 41, lines 21-36). As shown by Smithies et al., when the client
15 application and the transcript generator module both reside on the client system, then
16 the digital signatures will be attached at the client system.

17

18 Regarding claim 37, the combination of DeSimone et al. and Smithies et al.
19 discloses a program means for enabling attachment of a digital signature for a sender at
20 a messaging server before distribution to a plurality of participants (Smithies et al., Fig.
21 2, Col. 3, lines 40-61; Col. 9, lines 56-63; Col. 41, lines 21-36). As shown by Smithies
22 et al., the transcript generator module may reside on a system other than a client

Art Unit: 2137

1 system that has access to it. In this case, digital signatures from a plurality of
2 interacting client systems will be attached at the messaging server system.

3

4 Regarding claim 38, the combination of DeSimone et al. and Smithies et al.
5 discloses a program means for verifying at least one of an identity of a sender and an
6 integrity of content of said message entry (Smithies et al., Col. 9, line 64 – Col. 10, line
7 9; Col. 11, lines 44-67; Col. 13, lines 14-45; Col. 14, line 65 – Col. 15, line 4). As
8 disclosed by Smithies et al., a user via a client application can utilize the transcript
9 generator module to perform session verification functions upon the transcript, such as
10 verification of statements ('message entries') and their corresponding signatures.

11

12

13 Claims 6, 10, 14, 18, 22, and 26 are rejected under 35 U.S.C. 103(a) as being
14 unpatentable over DeSimone et al. in view of Smithies et al., as applied to claims 1, 9,
15 11, 17, 19, and 25 above, and further in view of Schneier, Applied Cryptography.

16

17 Regarding claim 6, the combination of DeSimone et al. and Smithies et al.
18 discloses a method, system, and program for recording a verifiable messaging session.
19 The messaging session comprises a plurality of users participating in the session. The
20 participating users are able to view the history of the messaging session in the form of a
21 'conversation', a string of recorded messages (DeSimone et al., Col. 2, lines 48-56; Col.
22 3, lines 43-53). They disclose the recording of a verifiable transcript of statements,

Art Unit: 2137

1 transactions, or events between parties by attaching digital signatures of the
2 participants to the transcript (Smithies et al., Col. 3, lines 40-61; Col. 41, lines 21-36).
3 Further more, they disclose a signature verification system for the verification of digital
4 signatures that are associated with a plurality of users who participate in the generation
5 of a messaging session (Smithies et al., Col. 9, line 64 – Col. 10, line 9; Col. 11, lines
6 44-67). The combination of DeSimone et al. and Smithies et al., however, does not
7 disclose the storing of the plurality of keys used by the signature verification system for
8 verifying the plurality of digital signatures belonging to the plurality of users.

9 Schneier discloses an authentication system using public-key cryptography
10 wherein a plurality of keys are stored for the verification of a plurality of digital
11 signatures belonging to a plurality of users (Pages 53 - 54). As disclosed by Schneier,
12 with public key cryptography, a host safely stores a plurality of keys that are used for
13 authentication ('verification') functions. Such keys must be safely stored so that they
14 may be used later for verification purposes.

15 It is obvious that any system utilizing public key cryptography to verify the digital
16 signatures of a plurality of users requires a system to manage the usage and storage of
17 such keys. Therefore, it would have been obvious to one ordinarily skilled in the art to
18 combine the method/system/program combination of DeSimone et al. and Smithies et
19 al. with the authentication/verification system of Schneier, because a
20 method/system/program that uses a plurality of public keys for verification requires a
21 system that manages and stores said keys.

22

Art Unit: 2137

1 Regarding claim 10, in view of the reasons given regarding claim 6, the
2 combination of DeSimone et al., Smithies et al., and Schneier discloses a method for
3 determining whether a public key received order to verify a particular digital signature
4 matches a public key coupled the particular digital signature; and in response to
5 determining a match, verifying a particular user associated with the particular digital
6 signature (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication system,
7 Schneier discloses the looking up of a particular public key coupled to a particular user,
8 and then using that key to decrypt a message. Thus, a determination has been made to
9 use the matching public key that is coupled to a user. In step 4, after performing a
10 successful decryption, the identity of the user is verified.

11

12 Regarding claim 14, in view of the reasons given regarding claim 6, the
13 combination of DeSimone et al., Smithies et al., and Schneier discloses a log file
14 repository for storing a plurality of public keys each associated with one from among a
15 plurality of digital signatures such that the plurality of public keys are accessible to a
16 plurality of users for verifying a messaging session (Schneier, Page 53).

17

18 Regarding claim 18, in view of the reasons given regarding claim 6, the
19 combination of DeSimone et al., Smithies et al., and Schneier discloses a system
20 means for determining whether a public key received order to verify a particular digital
21 signature matches a public key coupled the particular digital signature; and means for
22 verifying a particular user associated with the particular digital signature, in response to

Art Unit: 2137

1 determining a match (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication
2 system, Schneier discloses the looking up of a particular public key coupled to a
3 particular user, and then using that key to decrypt a message. Thus, a determination
4 has been made to use the matching public key that is coupled to a user. In step 4, after
5 performing a successful decryption, the identity of the user is verified.

6

7 Regarding claim 22, in view of the reasons given regarding claim 6, the
8 combination of DeSimone et al., Smithies et al., and Schneier discloses a program
9 means for enabling storage of a plurality of keys each associated with one from among
10 a plurality of digital signatures such that the plurality of public keys are accessible to a
11 plurality of users for verifying a messaging session (Schneier, Page 53).

12

13 Regarding claim 26, in view of the reasons given regarding claim 6, the
14 combination of DeSimone et al., Smithies et al., and Schneier discloses a program
15 means for determining whether a public key received order to verify a particular digital
16 signature matches a public key coupled the particular digital signature; and means for
17 verifying a particular user associated with the particular digital signature, in response to
18 determining a match (Schneier, Page 54, steps 1 – 4). In step 3 of the authentication
19 system, Schneier discloses the looking up of a particular public key coupled to a
20 particular user, and then using that key to decrypt a message. Thus, a determination
21 has been made to use the matching public key that is coupled to a user. In step 4, after
22 performing a successful decryption, the identity of the user is verified.

1

2 **Conclusion**

3

4 Any inquiry concerning this communication or earlier communications from the
5 examiner should be directed to Williams Jeffery whose telephone number is (571) 272-
6 7965. The examiner can normally be reached on 8:30-5:00.

7 If attempts to reach the examiner by telephone are unsuccessful, the examiner's
8 supervisor, Caldwell Andrew can be reached on (571) 272-3868. The fax phone
9 number for the organization where this application or proceeding is assigned is (703)
10 872-9306.

11 Information regarding the status of an application may be obtained from the
12 Patent Application Information Retrieval (PAIR) system. Status information for
13 published applications may be obtained from either Private PAIR or Public PAIR.
14 Status information for unpublished applications is available through Private PAIR only.
15 For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should
16 you have questions on access to the Private PAIR system, contact the Electronic
17 Business Center (EBC) at 866-217-9197 (toll-free).

18

Andrew Caldwell

19

20

21

22

23

24

**ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER**